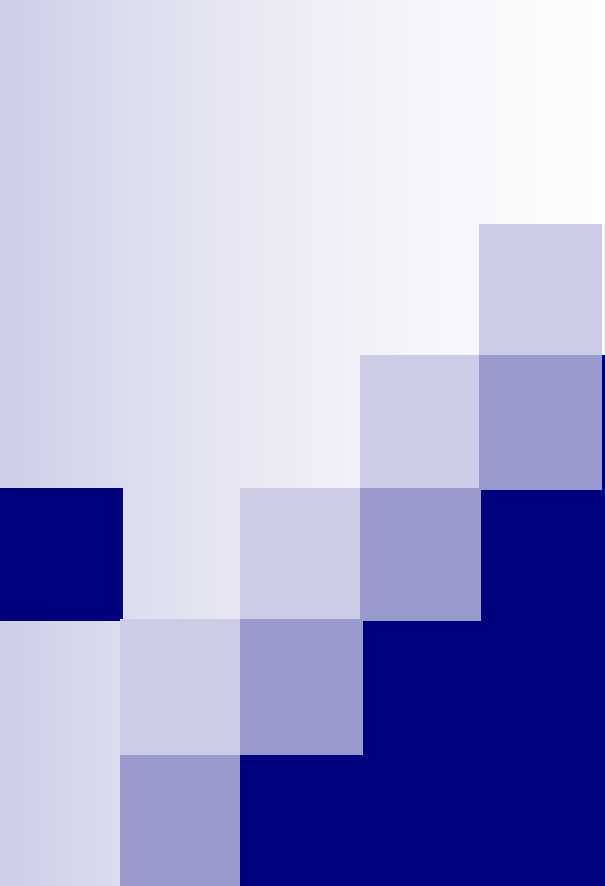


# ***Защита в операционных системах***

Вязанкин Олег Николаевич

к.ф.-м.н., доцент кафедры ПОЗИ, ИМИТ

[ovyazankin@gmail.com](mailto:ovyazankin@gmail.com)



## Тема 2. Основные типы угроз безопасности ОС и пути их реализации.



# План

- Основные определения
- Классификация угроз безопасности ОС
- Атаки на безопасность ОС

# Основные определения

- Под *угрозой* безопасности ОС будем понимать событие или действие, которое может вызвать изменение функционирования ОС, связанное с нарушением защищенности обрабатываемой в ней информации.
- *Уязвимость информации* – это возможность возникновения на каком-либо этапе жизненного цикла ОС такого ее состояния, при котором создаются условия для реализации угроз безопасности информации.
- *Атакой* на ОС будем называть действие, предпринимаемое нарушителем, которое заключается в поиске и использовании той или иной уязвимости. Иначе говоря, атака на безопасность ОС является реализацией угрозы безопасности информации в ней.

# Классификация угроз безопасности ОС

Универсальной классификации угроз не существует. Возможно, это связано с тем, что нет предела творческим способностям человека, и каждый день применяются новые способы незаконного проникновения в ОС, разрабатываются новые средства мониторинга сетевого трафика, появляются новые вирусы, находятся новые изъяны в существующих программных и аппаратных продуктах. В ответ на это разрабатываются все более изощренные средства защиты, которые ставят преграду на пути многих типов угроз, но затем сами становятся новыми объектами атак. Тем не менее, попытаемся сделать некоторые обобщения.

# Классификация угроз безопасности ОС

Классификация угроз *по цели атаки*:

- несанкционированное чтение информации;
- несанкционированное изменение информации;
- несанкционированное уничтожение информации;
- полное или частичное разрушение операционной системы (под разрушением операционной системы понимается целый комплекс разрушающих воздействий от кратковременного вывода из строя («завешивания») отдельных программных модулей системы до физического стирания с диска системных файлов).

# Классификация угроз безопасности ОС

Классификация угроз *по принципу воздействия на ОС:*

- использование известных (легальных) каналов получения информации, например, угроза несанкционированного чтения файла, доступ пользователей к которому определен некорректно – разрешен доступ пользователю, которому, согласно политике безопасности, доступ должен быть запрещен;
- использование скрытых каналов получения информации, например, угроза использования злоумышленником недокументированных возможностей операционной системы;
- создание новых каналов получения информации с помощью программных закладок.

# Классификация угроз безопасности ОС

Классификация угроз *по типу используемой злоумышленником уязвимости защиты*:

- неадекватная политика безопасности, в том числе и ошибки администратора системы;
- ошибки и недокументированные возможности программного обеспечения операционной системы, в том числе и так называемые люки – случайно или преднамеренно встроенные в систему «служебные входы», позволяющие обходить систему защиты; обычно люки создаются разработчиками программного обеспечения для тестирования и отладки, и иногда разработчики забывают их удалить или оставляют специально;
- ранее внедренная программная закладка.



# Классификация угроз безопасности ОС

Классификация угроз *по характеру воздействия на ОС:*

- активное воздействие — несанкционированные действия злоумышленника в системе;
- пассивное воздействие — несанкционированное наблюдение злоумышленника за процессами, происходящими в системе, и их последующий анализ.

Классификация угроз *по способу действий злоумышленника (нарушителя):*

- в интерактивном режиме (вручную);
- в пакетном режиме (с помощью специально написанной программы, которая выполняет негативные воздействия на операционную систему без непосредственного участия пользователя-нарушителя).

# Классификация угроз безопасности ОС

Классификация угроз *по способу воздействия на объект атаки*:

- непосредственное воздействие;
- превышение пользователем своих полномочий;
- работа от имени другого пользователя;
- использование результатов работы другого пользователя (например, несанкционированный перехват информационных потоков, инициированных другим пользователем).

# Классификация угроз безопасности ОС

Классификация угроз *по используемым средствам атаки*:

- штатные средства операционной системы без использования дополнительного программного обеспечения;
- программное обеспечение третьих фирм (к этому классу программного обеспечения относятся как компьютерные вирусы и другие вредоносные программы (exploits), которые можно легко найти в Internet, так и программное обеспечение, изначально разработанное для других целей: отладчики, сетевые мониторы, сканеры и т.д.);
- специально разработанное программное обеспечение.

# Классификация угроз безопасности ОС

Классификация угроз *по состоянию атакуемого объекта ОС на момент атаки*:

- хранение;
- передача;
- обработка.

Приведенная классификация не претендует ни на строгость, ни на полноту. Единственная ее цель – показать весь спектр возможных угроз безопасности ОС.

# Атаки на безопасность ОС

Операционная система может подвергнуться следующим типичным атакам:

■ **несанкционированный доступ.** Несанкционированный доступ (НСД) – наиболее распространенный вид компьютерных нарушений. Он заключается в получении пользователем доступа к объекту, на который у него нет разрешения в соответствии с принятой в организации политикой безопасности. Обычно самая главная проблема – определить, кто и к каким наборам данных должен иметь доступ;

■ **незаконное использование привилегий.** Злоумышленники, применяющие данный способ атаки, обычно используют штатное программное обеспечение, функционирующее в штатном режиме. Незаконный захват привилегий возможен либо при наличии ошибок в самой системе защиты (что, например, оказалось возможным в одной из версий *UNIX*), либо в случае халатности при управлении системой, и привилегиями в частности. Обычно это достигается путем запуска программы от имени другого пользователя. Строгое соблюдение правил управления системой защиты, соблюдение принципа минимума привилегий позволяет избежать таких нарушений;

# Атаки на безопасность ОС

- **сканирование файловой системы.** Злоумышленник просматривает файловую систему компьютера и пытается прочесть (или скопировать) все файлы подряд. Рано или поздно обнаруживается хотя бы одна ошибка администратора. В результате злоумышленник получает доступ к информации, доступ к которой должен быть ему запрещен;
- **подбор пароля.** Существует несколько методов подбора паролей пользователей:
  - тотальный перебор;
  - тотальный перебор, оптимизированный по статистике встречаемости символов или с помощью словарей;
  - подбор пароля с использованием знаний о пользователе (его имени, фамилии, даты рождения, номера телефона и т. д.);
- **кража ключевой информации.** Злоумышленник может подсмотреть пароль, набираемый пользователем, или восстановить набираемый пользователем пароль по движениям его рук на клавиатуре. Носитель с ключевой информацией (смарт-карта, Touch Memory и т. д.) может быть просто украден;

# Атаки на безопасность ОС

- **сборка мусора.** После окончания работы обрабатываемая информация не всегда полностью удаляется из памяти. Данные хранятся на носителе до перезаписи или уничтожения; при выполнении этих действий на освободившемся пространстве диска находятся их остатки. Хотя при искажении заголовка файла их прочитывать трудно, однако, используя специальные программы и оборудование, все же возможно. Такой процесс, который может привести к утечке важной информации, принято называть "сборкой мусора". Для защиты используются специальные механизмы. Примерами таких механизмов являются стирающий образец и метка полноты;

# Атаки на безопасность ОС

- **повторное использование объектов.** Повторное использование объектов (*object reutilization*) – состоит в восстановлении и повторном использовании удаленных объектов системы. Примером реализации подобного злоупотребления служит удаление файлов операционной системой. Когда ОС выдает сообщение, что некоторый файл удален, то это не означает, что информация, содержащаяся в данном файле, уничтожена в прямом смысле слова. Данное сообщение означает, что система пометила блоки памяти, ранее составлявшие содержимое файла, специальным флажком, говорящим о том, что данный блок не входит в состав какого-либо файла и может быть использован для размещения в нем другой информации. Но информация, которая была в данном блоке, никуда не исчезает до момента записи на это место другой информации. Таким образом, если прочесть содержание блока, можно получить доступ к "удаленной" информации;



# Атаки на безопасность ОС

- **люки.** Люки, или *trap door*, – не описанные в документации возможности работы с программным продуктом. Сущность использования люков состоит в том, что при реализации пользователем не описанных в документации действий он получает доступ к ресурсам и данным, которые в обычных условиях для него закрыты (в частности, вход в привилегированный режим обслуживания).
  - Люки чаще всего являются результатом забывчивости разработчиков. В процессе разработки программы создаются временные механизмы, облегчающие ведение отладки за счет прямого доступа к продукту (например, вирус Морриса в ОС UNIX).
  - Люки могут образоваться также в результате часто практикуемой технологии разработки программных продуктов сверху вниз. При этом программист приступает к написанию управляющей программы, заменяя предполагаемые в будущем подпрограммы так называемыми заглушками – группами команд, имитирующими или обозначающими место присоединения будущих подпрограмм. В процессе работы эти заглушки заменяются реальными подпрограммами. На момент замены последней заглушки реальной подпрограммой программа считается законченной. Но на практике подобная замена выполняется не всегда;

# Атаки на безопасность ОС

- **отказы в обслуживании.** Несанкционированное использование компьютерной системы в своих целях (например, для бесплатного решения своих задач), либо блокирование системы для отказа в обслуживании другим пользователям. Для реализации такого злоупотребления используются программы, способные захватить монопольно определенный ресурс системы (причем необязательно центральный процессор). В последнее время большое распространение получили атаки класса "отказ в обслуживании", так называемые *распределенные атаки*, приводящие к тому, что Web-серверы кредитно-финансовых учреждений оказываются перегруженными ложными запросами и не могут обслуживать клиентов. В последнее время эти атаки приобрели большую популярность. Злоумышленник может реализовать посылку большого объема данных сразу из всех узлов, которые задействованы в распределенной атаке. В этом случае атакуемый узел захлебнется огромным трафиком и не сможет обрабатывать запросы от нормальных пользователей;

# Атаки на безопасность ОС

- **работа между строк.** Работа между строк (*between lines*) – подключение к линиям связи и внедрение в компьютерную систему с использованием промежутков в действиях законного пользователя. При интерактивной работе пользователя образуются своеобразные окна (например, отклик системы опережает действия пользователя, которому необходимо время для обдумывания последующих действий). Эти окна вполне могут быть использованы нарушителем для работы с системой под маской пользователя;
- **анализ трафика.** Анализ трафика (*traffic analysis*) – специализированная программа анализирует проходящий по сети трафик и декодирует его, в результате чего можно получить большой объем информации: топологию сети, о пользователях, работающих в настоящий момент в сети, пароли пользователей и т.д.;

# Атаки на безопасность ОС

- **"подкладывание свиньи":** "Подкладывание свиньи" (*piggyback*) – нарушитель подключается к линиям связи и имитирует работу системы с целью осуществления незаконных манипуляций. Например, он может имитировать сеанс связи и получить данные под видом легального пользователя. Пользователь, не подозревая об этом, передает информацию и (или) получает ее. Таким образом может осуществляться не только шпионаж, но и дезинформация, что также отрицательно сказывается на работе системы и объекта управления в целом.

# Атаки на безопасность ОС

В последнее время участились случаи воздействия на вычислительную систему при помощи специально созданных программ. Для обозначения всех программ такого рода был предложен термин "**вредоносные программы**» (*malicious software*). Эти программы прямо или косвенно дезорганизуют процесс обработки информации или способствуют утечке или искажению информации. Рассмотрим самые распространенные виды подобных программ.

■ **Вирус** (*viruses*) – это программа, которая способна заражать другие программы, модифицируя их так, чтобы они включали в себя копию вируса. Когда такой исполняемый код загружается в оперативную память для выполнения, вместе с ним получает возможность исполнить свои вредительские действия вирус. Вирусы могут привести к повреждению или даже полной утрате информации.

■ **"Червяки"** (*worms*) – это программы, которые распространяются в системах и сетях по линиям связи. Такие программы подобны вирусам в том, что заражают другие программы, а отличаются от них тем, что не способны самовоспроизводиться.

# Атаки на безопасность ОС

- **"Троянский конь"** (*Trojan horses*) – это программа, которая приводит к неожиданным (обычно нежелательным) результатам. Особенностью этих программ является то, что пользователь обращается к этой программе, считая ее полезной. Программа-"троянский конь" всегда маскируется под какую-нибудь полезную утилиту или игру, а производит действия, разрушающие систему. "Троянские кони" способны раскрыть, изменить или уничтожить данные или файлы. Их встраивают в программы широкого пользования, например в программы обслуживания сети, электронной почты. Реализация дополнительных функций выполняется скрытым от пользователя модулем, который может встраиваться в системное и прикладное программное обеспечение. При реализации пораженной программы "троянский конь" получает доступ к ресурсам вместе с пользователем. Компьютерные системы, использующий дескрипторные методы управления доступом (в том числе такие, как полномочия, списки управления доступом и др.), становятся практически беззащитными против программ типа "троянский конь".

# Атаки на безопасность ОС

- **жадные программы** – это программы, преднамеренно захватывающие значительную часть ресурсов компьютера, в результате чего другие программы не могут выполняться или выполняются крайне медленно. Запуск жадной программы может привести к краху операционной системы.
- **"Бактерия" (*bacteria*)** – программа, которая делает копии самой себя и становится паразитом, перегружая память и процессор.
- **Репликаторы** – могут создавать одну или более своих копий в компьютерной системе. Это приводит к быстрому переполнению памяти компьютера, но данные действия могут быть обнаружены опытным пользователем и достаточно легко устранены. Устранение программы репликатора усложняется в тех случаях, когда репликация выполняется с модификацией исходного текста программы, что затрудняет распознавание ее новых копий. Репликаторные программы становятся особенно опасными, когда к функции размножения будут добавлены другие разрушающие воздействия.

# Атаки на безопасность ОС

- **"Захватчик паролей"** (*password grabber*) – программы, специально предназначенные для получения идентификаторов и паролей пользователей. Программы открытия паролей последовательно генерируют все возможные варианты пароля и выдают их системе до тех пор, пока не будет определен необходимый пароль. Пароли являются основным средством идентификации пользователей в многопользовательских компьютерных системах, и открытие пароля и входного имени пользователя позволяет организовать доступ к конкретной информации. Программы захвата паролей имитируют различные события в ИС, например системный сбой в работе компьютера (перезагрузку операционной системы, отключение сети и др.), и запрашивают у пользователя идентификатор и пароль, после чего передают управление рабочей программе, операционной системе или другим программам.



# Атаки на безопасность ОС

- **"Логические бомбы"** (*logic bombs*) – программа, которая приводит к повреждению файлов или ОС (от искажения данных до полного уничтожения данных). "Логическую бомбу" вставляют, как правило, во время разработки программы, а срабатывает она при выполнении некоторого условия (время, дата, кодовое слово). "Логические бомбы", в которых срабатывание скрытого модуля определяется временем (текущей датой), называют бомбами с часовым механизмом (*time bomb*). Подобные программы реализуют свой механизм после конкретного числа исполнений при наличии или, наоборот, отсутствии определенного файла, а также соответствующей записи в файле. В связи с тем что подобные программы имеют ограниченный доступ к ресурсам системы, разрушительный эффект остается достаточно низким. Опасность может значительно увеличиться, если "логическая бомба" будет встроена в системное программное обеспечение, что приведет к уничтожению файлов, переформатированию машинных носителей или к другим разрушающим последствиям. Основной целью функционирования программ типа логической бомбы следует считать нарушение нормальной работы компьютерной системы.

# Атаки на безопасность ОС

- **Программные закладки** – скрытно внедрённая в защищенную систему программа, либо намеренно измененный фрагмент программы, который позволяет злоумышленнику осуществить несанкционированный доступ к ресурсам системы на основе изменения свойств системы защиты. Закладка может быть внедрена самим разработчиком программного обеспечения. Часто программные закладки выполняют роль перехватчиков паролей, трафика, а также служат в качестве проводников для компьютерных вирусов. Программные закладки невозможно обнаружить при помощи стандартных антивирусных средств, их выявление возможно только специальными тестовыми программами. Данные программы доступны в специализированных компаниях, которые занимаются сертификацией и стандартизацией компьютерного программного обеспечения.

Необходимо отметить, что при планировании и разработке злоупотреблений нарушителями могут создаваться новые, не приведенные в данной классификации, а также применяться любые сочетания описанных злоупотреблений.